TN Department of General Services

MEMO

SWC# 3999 NASPO COTS Software
Contract Information and Usage Instructions

STS CONSOLIDATED EXECUTIVE BRANCH AGENCIES
All software from this contract must be requested through ServiceNow if STS personnel will be installing & supporting the software. Non-STS supported software and all professional services may be ordered directly in Edison by procuring agency.

Contract Period
Start Date: January 1, 2023
Final End Date with all Annual Renewal Options: April 24, 2027

Summary/Background Information
Statewide contract 3999 scope of offerings include Commercial Off-the-Shelf (COTS) Software and maintenance, along with software services that include installation/implementation, development, consulting, training.

To find the list of select software titles eligible for purchase under this statewide contract, please visit the links below. Please contact the vendor regarding additional software titles that are not itemized but are available through the contract.

CDW-G: https://www.naspovaluepoint.org/portfolio/software-var/cdw-g/
Dell Marketing: https://www.naspovaluepoint.org/portfolio/software-var/dell-marketing/
Insight: https://www.naspovaluepoint.org/portfolio/software-var/insight/
SHI: https://www.naspovaluepoint.org/portfolio/software-var/shi/
Zones: https://www.naspovaluepoint.org/portfolio/software-var/zones/

Statements of Work
Please use a statement of work (SOW) when your purchase includes consulting services. We have created a SOW template for your use, see Attachment 1 below.

Security Requirement Rider
This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either as an attachment to the SOW (refer to Attachment 1 below) or printed on to the purchase order directly if no SOW is being used. STS Information Security will review the type(s) of data being hosted and will designate what additional applicable terms and conditions will apply to the purchase.

Out of Scope Services
Custom/Customized software licensing developed by a vendor solely for the State of TN.

Category 1 - Software Value-Added Reseller ('Reseller' – "SVAR") – All Publishers Excluding Microsoft and Oracle Software | Out of Scope Products - Non-SaaS cloud computing products such as Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Software

provided by a Managed Services Provider are generally out of scope of this Contract. IaaS shall be allowable only as an incidental product when 1) SaaS is the primary and predominate title being purchased, and 2) the limited and incidental licensing of the publisher's IaaS is essential to the successful and efficient implementation and or deployment of the SaaS software. This determination should be made by the purchasing entity in advance of any IaaS purchase.

Category 2 – Microsoft SVAR | Out of Scope Products - Non-SaaS cloud computing products such as Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Software provided by a Managed Services Provider are generally out of scope of this Contract. IaaS shall be allowable only as an incidental product when 1) SaaS is the primary and predominate title being purchased, and 2) the limited and incidental licensing of the publisher's IaaS is essential to the successful and efficient implementation and or deployment of the SaaS software. This determination should be made by the purchasing entity in advance of any IaaS purchase.

STS Consolidated Agencies
To enter a request for STS to procure software for your agency, please submit a ServiceNow Software Procurement Request via the link below.
https://tn.service-now.com/sp?id=sc_cat_item&sys_id=8775167a13826a009f84b6246144b071

STS Software Waiver / Exception Process
To request a waiver or exception to a standard product, a policy or a standard that is currently included in the Tennessee Enterprise Architecture, submit a ServiceNow Standard Product List Exception Request through the following link:
https://tn.service-now.com/sp?id=sc_cat_item&sys_id=a7c7b338db4d4510b09ccde813961953

Onboarding Publishers to NASPO Statewide Contracts (SWC)
Publishers need to be partnered with a contract reseller to be available for purchase. If a publisher is available through the reseller under the contract, the State can purchase from the publisher immediately upon receiving a quote from the contract reseller.

To onboard a publisher with available contract resellers:

1. Determine/confirm publisher point of contact
2. Inform the publisher of the State's intent to have them added to the SWC. Give the publisher the contact information of the contract resellers that will be reaching out. Explain that the State does not have a preference on which contract reseller the publisher executes a partnership agreement.
3. Email contract resellers to request the publisher be onboarded and provide the publisher contact information to the reseller. Current reseller contact information is below:
    a. Insight - TeamAshley2@Insight.com, Ashley.McDonald@Insight.com
    b. SHI - southeastteamgov@shi.com, nick_porco@shi.com, lexi_ettman@shi.com
    c. CDW) -heather.kohls@cdwg.com
    d. (Dell) - TBD
    e. Zones - NASPO-SVAR@zones.com
4. Coordinate between publisher and contract resellers to facilitate the onboarding process. Coordination tasks could include facilitating communication between the publisher and resellers, ensuring the publisher/resellers continue to prioritize the onboarding process, and answering questions from the publisher/resellers or connecting the appropriate State contacts to provide guidance to the publisher/resellers.

5. Once onboarding is complete, the State can purchase the publisher's licensing and services through their partnered resellers.

State Contact Information

Contract Administrator	STS Business Operations
Zohreh Hurd	Joyanna Brassfield
Central Procurement Office	Strategic Technology Solutions
615-741-2026	(615) 313-5434
zohreh.hurd@tn.gov	joyanna.brassfield@tn.gov
	Additional STS Business Operations Team Contacts: https://www.teamtn.gov/sts/all-services/sts-business-operations-procurement/contacts.html

Vendor Contact Information:

Company Name: CDW-G
Master Agreement #: ADSPO16-130652
Edison Contract Number: 77273
Vendor Number: 534
Heather Kohls, Manager, Program Management heather.kohls@cdwg.com (847) 465-6000

Company Name: Dell Marketing
Master Agreement #: TBD
Edison Contract Number: TBD
Vendor Number: TBD
TBD

Company Name: Insight
Master Agreement #: ADSPO16-138244
Edison Contract Number: 77151
Vendor Number: 529
*All emails, purchase orders, quote requests and communications are required to be sent to teamashley2@insight.com Ashley McDonald, Account Executive – Field Sales ASHLEY.MCDONALD@INSIGHT.COM 423.368.9042 teamashley2@insight.com Branden Maiorano, Associate Account Executive – Quotes & Order Status BRANDEN.MAIORANO@INSIGHT.COM 737.247.3702

Molly Randol, SLED Business Development Mngr. – Onboarding Contracts
molly.randol@insight.com 480.902.1086

Jason Williams, Microsoft Support
Jason.williams@insight.com 501.505.4742

Company Name: Software House International (SHI)
Master Agreement #: ADSPO16-130651
Edison Contract Number: 77158
Vendor Number: 12676
Quote requests: TennesseeTeam@SHI.com Nick Porco, Account Executive Nick_Porco@shi.com

Company Name: Zones
Master Agreement #: CTR060031
Edison Contract Number: 77343
Vendor Number: 263880
Quote requests: NASPO-SVAR@zones.com

Key Contract Information

All Master Price Agreements and baseline offerings can be found on the NASPO website, under the Contractors tab: https://www.naspovaluepoint.org/portfolio/software-var/

Billing and Payment Instructions:
Follow your agency specific rules for bill and payments.
Net payments term: **Net 30**

NASPO ValuePoint Background Information:

NASPO ValuePoint (formerly known as WSCA-NASPO) is a cooperative purchasing program of all 50 states, the District of Columbia and the territories of the United States. The Program is facilitated by the NASPO Cooperative Purchasing Organization LLC, a nonprofit subsidiary of the National Association of State Procurement Officials (NASPO), doing business as NASPO ValuePoint. NASPO is a non-profit association dedicated to strengthening the procurement community through education, research, and communication. It is made up of the directors of the central purchasing offices in each of the 50 states, the District of Columbia and the territories of the United States. NASPO ValuePoint facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. For more information consult the following websites: www.naspovaluepoint.org and www.naspo.org

ATTACHMENT 1

SWC# 3999 NASPO COTS Software

[Insert Department Name]

Statement of Work
SOW ID # xxxx-xxxx

For

[Insert Project Title]

[SOW Start Date]

Contents

1.0 Statement of Work

1.1 *Project Title*

This Statement of Work (SOW) is being executed between *[insert Contractor name]* ("Contractor") and *[Insert Agency]* ("State") for [*insert a brief description of the project*], effective as of *[Insert Effective Date]* (the "SOW Effective Date").

- *Update/include this subcontractor language below in the event of this SOW project utilizes subcontractors.*

[Subcontractor name] (xx) shall act as a "Subcontractor" to [Contractor Name] ("Contractor") to perform the requested professional services. When references are made to the "Contractor" performing work under this SOW, this shall be construed to mean that the work is performed by Subcontractor. However, the Subcontractor is not a signatory to this SOW, and the Contractor shall be fully responsible for the successful execution of all requested services
This SOW constitutes an Order under applicable Participating Addendum between the Contractor and the State, via Edison Contract # xxxxx (the "Contract") and incorporates by reference the terms and conditions, specifications, and other incorporated contract documents of the Contract. In case of any conflict between this SOW and the Contract, the Contract shall prevail.

1.2 Background

- *Describe the history of your project and the prior events that brought you to this SOW*

1.3 Reference to other applicable documents
The following documents are hereby incorporated by reference into this SOW:

- *List any pertinent documents or supporting materials pertaining to the SOW, if any, otherwise write "None".*

1.4 Definitions

1.5 Security, Audit, and Other Requirements –

a. Security Requirement Rider

The State's confidential data and security requirements ("Requirements") are contained in the SWC# 3999 NASPO COTS Software Participating Addendum (PA) and have been agreed to by the participating Contractors to comply with during a SOW project.

To bring attention to the specific Requirements the Contractor shall provide and comply with during the SOW project in question, a Security Requirement Rider will be included as an attachment to this SOW.

The Security Requirement Rider, SOW Attachment 2 contains the full version of the Contractor Hosted Services Confidential Data, Audit, and Other Requirements terms and conditions included in the SWC# 3999 NASPO COTS Software Participating Addendum (PA).

Additional Operational Security Requirements are listed in Attachment 2 Section 2.

NOTE: The applicable security Requirements will be dependent upon the type(s) of data associated with the project requirements and deliverables outlined in this SOW.

2.0 STATE STAFFING AND ROLES

2.1 Staffing

Project Manager – State
The State's Project Manager is:

Name:
Address:
City:
State & Zip
Phone:
Cell:
Fax:
Email:

Insert contact information for any additional relevant staff.

Contractor's Point of Contact is:

Name:
Address:
City:
State & Zip
Phone:
Cell:
Fax:
Email:

2.2 State Staff and Roles:

- *Who within the State will have decision-making authority, including approval of changes, report, documentation, and deliverables?*
- *State staff (if any) to assist with the project effort*
- *Individuals key to the project and detail their roles and responsibilities*

2.3 Contractor Staff and Roles:

- *Who from the Contractor will have decision-making authority, including approval of changes, report, documentation, and deliverables?*
- *Contractor staff (if any) to assist with the project effort*
- *Individuals key to the project and detail their roles and responsibilities*

3.0 PROJECT REQUIREMENTS AND DELIVERABLES

3.1 Contractor Requirements and Deliverables

3.1.1 Requirements:

- *Tasks to be performed and any additional Contractor qualifications for specialized projects*
- *Any known non-standard work schedule tasks*
- *Location(s) where project work is required to be performed or may be performed, including the use of onsite, offsite, and offshore resources at the procuring State's discretion*
- *Include tasks that do not result in specific deliverables (i.e. project management)*
- *Include any security requirements from Special Terms and Conditions, Section 13 of the Contract that are applicable to this SOW.*

3.1.2 Deliverables

- *Describe the Deliverables to be provided under this SOW, including the estimated delivery dates. If no Deliverables, state "none.*

3.2 State Tasks and Responsibilities

- *Include tasks to be performed by the State*
- *Precise definition of all hardware, software, data services, and facilities the State will provide*

3.3 Exclusions

Describe:

- *Tasks which are not part of the scope of this project*

4.0 DELIVERABLE ACCEPTANCE

The State will review/validate each deliverable and provide either written acceptance of the deliverable or written rejection of the deliverable including a detailed list of deficiencies that must be remedied prior to approval of the deliverable. In the event the State notifies the Contractor of deficiencies, the Contractor shall make necessary corrections within a specify period of time (or "timeline mutually agreed upon"), mutually agreed upon between State and Contractor. Deliverables can only be accepted by an authorized State representative per Section 2.1.

a. Following delivery of a Deliverable by the Contractor, the State will promptly review, and inform the Contractor in writing of State's acceptance or rejection of such Deliverable based on compliance in all material respects with the applicable specifications. Any rejection by the State must specify the material deficiencies of such Deliverable. If State fails to accept or reject such Deliverable within **10** business days after delivery, the Deliverable will be deemed accepted. Upon receipt of a corrected Deliverable from the Contractor, the State will have an additional period of time, not to exceed **10** business days, to review the corrected Deliverable to confirm that the material deficiencies have been corrected.

Define the process for submitting, approving and rejecting deliverables (including testing dates

and scenarios)

5.0 COST CRITERIA

5.1 Payment Methodology

Describe the payment methodology and the associated charges applicable to this SOW.

5.2 SOW Monetary Cap

Check one of the following to apply to this SOW:

- ☐ This SOW is a fixed fee SOW. The total charges under this SOW is *[_____]* dollars *($___) [specify SOW monetary cap]* for the performance of the work as set forth in this SOW.

- ☐ This SOW is a time and materials SOW. The total charges under this SOW is *[_____]* dollars *($___) [specify SOW monetary cap]* for the performance of the work as set forth in this SOW (the "SOW NTE Amount"). The State shall compensate the Contractor for actual work performed, in an amount not to exceed the SOW NTE Amount. The State shall not be obligated to pay for, and the Contractor shall not be obligated to perform, work under this SOW in excess of the SOW NTE Amount unless and until the parties execute a written revision to this SOW to increase such SOW NTE Amount.

- ☐ This SOW is a consumption-based SOW. The estimated charges under this SOW is *[_____]* dollars *($___) [specify SOW estimated budget]*. For clarity, the terms of this SOW and the Contract will continue to apply to any Cloud Services provided in excess of the specified estimated charges.

Position Description	***Hourly Rate****	***Number of Hours***	***Cost***
Position Name			
Position Name			
Position Name			
Position Name			
Position Name			
Position Name			
Position Name			
Position Name			
TOTAL Fees			

* Hourly Rates should be equal to or less than the rates agreed to in the Contractor's Master Agreement.

5.3 State Billing Address

Insert the applicable State billing address.

6.0 ESTIMATED TIMELINE AND PERIOD OF PERFORMANCE

Project must begin no later than *[Month, Year]* and be completed by *[Month, Year]*.

Optional Milestone Table

Milestone	Date

7.0 PROJECT MANAGEMENT (*IF APPLICABLE*)

Describe what will be required as far as project management, which reports will be required, how often these reports will be required, and what must be submitted to the State.

8.0 ADDITIONAL STATE POLICIES AND STANDARDS

Specifically reference any additional state policies and standards that would apply, to the extent applicable to Contractor in its performance of the work under the Order. If none, write "none".

- *Insert any other relevant links to the latest versions of the policies, standards and environment*

9.0 KEY ASSUMPTIONS

Identify any additional State or contractor assumptions

If additional sections are required for your specific project, please leave the above section numbering as it is and add your new sections here as 10.0, 11.0 etc.

10.0 SOW Revision Procedure

The State may request necessary changes to the deliverables and requirements due to policy or operational changes during the SOW term. The Contractor shall address these necessary changes as per the SOW revision procedures described in this section.

10.1 The State shall provide to the Contractor a written request for changes. After receipt of the written request, the Contractor shall respond to the State with a written proposal for implementation of the change. The written proposal must include the following:

a) Complete description of the work to be performed as the Contractor understands it,

b) Work plan showing the major activities needed to complete the necessary change, including adjustment to the schedule and tasks required, and

c) Provide a “not to exceed” total cost for the work in question. The State shall pay no more than, and the Contractor will not be required to provide services in excess of, this cost for the services engagement. The Contractor shall provide supporting documentation which lists the number of hours and materials, if applicable, that constitute the “not to exceed” cost.

10.2 The State shall review the Contractor’s written proposal and approve or request additional clarification for approval. If approved, the agreed to changes will be documented in the State’s standard SOW revision template.

10.3 The Contractor and the State shall sign the SOW revision template. Once executed by the Contractor and the State, the SOW , shall be binding to both parties. and it shall constitute an revision between the SOW parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this SOW.

10.4 The SOW revision shall not conflict with, modify, or delete the terms and conditions of the SOW or Contract. In the event of a conflict or ambiguity between the Contract, SOW, and this SOW amendment, the Contract, then the SOW shall prevail, in that order.

10.5 SOW amendments shall not contain any other legal terms and conditions that modify, contradict, or supplement the terms of the SOW or Contract. Any such terms and conditions
contained in a SOW revision shall be void, invalid, and unenforceable against the State.

This SOW will not be effective, and Contractor shall not commence services hereunder, until it is approved and signed by Contractor and the Participating Entity.

In witness whereof, the parties have executed this SOW as of the last date of execution of the signatories below.

[Insert State Purchasing Agency]	*[Contractor Name]*
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Optional SOW Language

- Key Assumption language:
  - The Contractor shall procure a State approved laptop device. A basic State image shall be installed on the device prior to shipment. Once received by the Contractor, the State will remotely install all required software applications and tools to be in compliance with the State's Information Security Policy. At the end of the SOW, the Contractor shall permit the State to remotely access the devices in order to delete all data from the devices. Cost of the devices must be included as a part of the monthly services fee.
- Project Management language:
  - The State reserves the right to request personnel changes to the Contractor project team if it is determined that performance does not meet State's expectations. If personnel changes are necessary, the Contractor shall replace assigned personnel with equal or higher skills and meets the requirements defined in section 3 to the personnel who are replaced. The Contractor must submit resumes of replacement personnel within five (5) business days of State notification.
  - If the Contractor fails to provide equally qualified candidates, the State reserves the right to terminate the SOW contract with selected Contractor.
- Section 3 requirement language:
  - Acceptance testing of Functional Deliverables during UAT will involve the validation of each Functional and Successfully Operating Deliverable against the Approved State Specifications. The acceptance period for the Functional Operating Deliverable will be **10** business days. If the Functional and Successfully Operating Deliverable conforms to the Approved State Specifications, it will be accepted. If not, then any Material Nonconformities will be:

    X. fed by Subcontractor into list of identified defects or product backlog and;
    X. prioritized by the State and mutually agreed by both Parties to be addressed as part of the scope of services defined in the SOW or deferred for future consideration. Contractor/Subcontractor's correction efforts will be made on a time and materials basis. If Contractor/Subcontractor does not receive notice identifying a Material Nonconformity from State during acceptance period or State begins using the Functional and Successfully Operating Deliverable in a production environment, or the acceptance period expires, the Functional and Successfully Operating Deliverable shall be deemed to be accepted.

ATTACHMENT 2

Security Requirement Rider
Applicable Security Terms and Conditions
and Operational Requirements

Internal Instructions: *After the STS Security team determines what requirements are required for a specific SOW, this attachment will be revised, through a subtractive process, to contain only the corresponding full version text of the Pick List requirement in SOW Section 1.4 and will then be attached to the SOW.* **(Delete instructions before adding the Attachment to the SOW)**

This Security Requirement Rider contains the full version text of the data confidentiality and data security terms and conditions found in the SWC# 3999 NASPO COTS Software PA Section, Contractor Hosted Services Confidential Data, Audit, and Other Requirements that shall be applicable for this SOW.

These terms and conditions are also located in each of the NASPO COTS Software Contractor's Participating Addendum (PA).

Please note pre-existing global security language exists in the resellers PA; therefore, it is unnecessary to repeat the language in this rider.

1. Contractor Hosted Services Confidential Data, Audit, and Other Requirements.

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

1. The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

2. The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.

3. The Contractor and the Contractor's processing environment containing

Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO")
27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with
the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the
State with the Contractor's and Subcontractor's annual SOC Type II audit

report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action
plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating
whether the Contractor or Subcontractor made any material changes to their
control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Estimated Liability of this Contract.

Contractor shall meet all applicable requirements of the most current version of Internal Revenue Service Publication 1075.

Contractor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges ("MARS-E") controls.

(a) If the order will involve CJIS data, or FTI data then the following shall apply in lieu of section 14.a.(3):

The Contractor shall maintain a Security Management Certification from the Federal Risk and Authorization Management Program ("FedRAMP"). A "Security Management Certification" shall mean written confirmation from FedRAMP that FedRAMP has assessed the Contractor's information
technology Infrastructure, using a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, and has certified that the Contractor meets FedRAMP
standards. Information technology "Infrastructure" shall mean the Contractor's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services. The Contractor
shall provide proof of current certification annually and upon State request. No additional funding shall be allocated for these certifications,
authorizations, or audits as these are included in the Estimated Liability of this Contract.

b. If the order will contain FTI data, the following sentence also applies to section 14.a.(3)(a) (FedRAMP) language above:

Contractor shall meet all applicable requirements of the most current

version of Internal Revenue Service Publication 1075.

c. If the order will involve CMS data, the following sentence also applies to section 14.a.(3)(a) language above:

Contractor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges ("MARS-E") controls.

4. The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

5. Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.

6. Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

(7) If the order will involve PCI data, the following shall apply:
Contractor shall be certified to host Payment Card Industry ("PCI") data in accordance with the current version of PCI DSS ("Data Security Standard"), maintained by the PCI Security Standards Council.

b. Minimum Requirements

(1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html.

2. The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

3. If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

1. "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: The applicable RPO will be defined in each Order.

ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: The applicable RTO will be defined in each Order.

2. The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

3. The Contractor shall have the ability to provide base level protection against Layer 3 and Layer 4 Distributed Denial of Service volume based and protocol attacks such as SYN, UDP, and ICMP floods, DNS amplification and reflection attacks.

4. The contractor shall have the ability to provide addition mitigation against Layer 7 Distributed Denial of Service attacks such as HTTP floods, WordPress XML-RPV Floods and Slowloris attacks.

d. In the event of a cyber breach, the Contractor will allow the State to communicate directly with the Contractor's technical staff and any forensics experts who are assisting the Contractor with the breach analysis.